

Universidad Carlos III de Madrid
Telematic Engineering Department

Computer Networks

Practice – Traffic interception and data analysis

Bachelor in Informatics Engineering

1. Objective

The main objective of this practice is to deepen the understanding of the most important protocols from TCP/IP model seen in the subject. To do this, you will use various applications that implement them, and the traffic capture / packet sniffer (Wireshark - <http://www.wireshark.org/>) used in the concept practice no. 1 (DNS).

2. Description

Throughout this practice you will deepen fundamental concepts of protocols at different levels of TCP/IP model. Specifically, transport, network and link layers will be studied. In the link layer we will focus on Ethernet and ARP. For the network layer, the analysis will be performed on IPv4. Finally for the transport layer, TCP characteristics will be studied.

In order to do this practice in an easy way, there have been chosen some existing applications, both in GNU Linux and Microsoft Windows. Note that you can do the practice on both operating systems, but commands may vary depending on the OS.

The practice has been divided into a couple of independent parts, which are distributed among a series of tests for each of the layers outlined above.

2.1. Part I [Transport and network layers]

IMPORTANT: The document in which to answer the questions must be submitted **no more than 10 minutes** after completion of the **first capture session** through the “*Delivery 1. Wireshark*” configured for that purpose in Aula Global 2.

2.1.1. – Transport layer

In this section we are going to analyze the one of the main transport protocols used in the Internet: the *Transmission Control Protocol* (TCP). Follow the next steps:

- 1.- Open Wireshark and start a capture session using the correct network interface.
- 2.- Open **one** of the following web addresses: <http://goo.gl/wFwVD> or <http://goo.gl/grDQf>
- 3.- Let the video play.
- 4.- After some seconds (**less than a minute**) stop the capture session.

Answer the following questions:

P1) Identify the messages for the “tree-way-handshake” process. What information is exchanged in each of them? What are the sequence numbers and ACK for each message? Attach a screenshot.

P2) Identify the first message sent after “three-way-handshake”. What are the source IP address and port of the message? And what are the destination IP and port? What SEQ Num. does the message have? What will be the expected ACK number for this message?

P3) What is the transport protocol (TCP or UDP) used to send the video stream? Why do you think they do in this way?

P4) Identify the first message sent in the video stream download. What is the IP address of the remote server? What is the destination port? And the source port? Attach a screenshot.

P5) Select one captured packet which belongs to the video stream and generate the “Throughput” graph corresponding to this stream (Statistics → TCP Stream Graph → ...). Attach a screenshot and write why you think it has this shape.

About the graph generated in P5:

P6) How long the PC has been receiving the video stream? (Not playing video but receiving the stream!!!. Approximate amount of time).

P7) What is the average video download speed? This rate has been constant along the download or not? Why do you think that? Justify all the answers.

2.1.2. – Network layer

In this section we are going to analyze one of the main protocols in the network layer, the *Internet Protocol (IP)*. More specifically IPv4. Follow the next steps:

- 1.- Open Wireshark and a command prompt (or Shell under GNU Linux).
- 2.- In the command prompt write the command to do a ping to the default Gateway of your host. (this is, the router IP address which gives Internet access to the host). **Do not execute it yet!**
- 3.- Using Wireshark start a capture session using the correct network interface.
- 4.- In the command prompt execute the previous command.
- 5.- After capturing several ping messages, stop the capture.

P1) What is the ICMP message total size? How much data is sent in the ICMP message? Describe how much space is used by each part of the message (headers, data, etc.).

P2) What are the source and destination ports of the ICMP message? Why do you think this? Justify all your answers.

Repeat the previous steps, but this time send **60000 bytes** in each message. Answer the following questions:

P3) Explain in detail how the results have changed now with respect to the previous test.



P4) Find the fragment with the ICMP message header (attach a descriptive snapshot).

P5) Why no response is received until destination received all the fragments instead of replying fragment by fragment?

P6) What does data field content? Specify the OS used to do this test.

2.2. Part II [Link layer]

IMPORTANTE: The document in which to answer the questions must be submitted **no more than 10 minutes** after completion of the **second capture session** through the “*Delivery 2. Wireshark*” configured for that purpose in Aula Global 2.

2.2.1. Ethernet

In order to answer the questions, follow the next steps:

- 1.- Open Wireshark and a command prompt (or Shell under GNU Linux).
- 2.- In the command prompt write the command to do a ping to the default Gateway of your host. (this is, the router IP address which gives Internet access to the host). **Do not execute it yet!**
- 3.- Using Wireshark start a capture session using the correct network interface.
- 4.- In the command prompt execute the previous command.
- 5.- After capturing several ping messages, stop the capture

Answer the following questions:

P1) What are the source and destination MAC addresses in the ICMP message?

P2) Can you see the gateway IP address in the message? And its MAC address? Justify all the answers.

P3) What does mean the Ethernet layer flags in the ICMP message?

Repeat the steps 1 to 5, but this time ping www.google.com. Answer the following questions:

P4) What are the source and destination MAC addresses in the ICMP message?

P2) Can you see the Google IP address in the message? And its MAC address? Justify all the answers.

2.2.2. ARP

*P6) Obtain ARP table of the host by using **arp** command. Describe the fields shown and attach a screenshot.*

Follow the next steps:

- 1.- Open Wireshark and start a capture session using the correct network interface.
- 2.- Ping www.google.com.

3.- Stop the capture session after intercepting some ping messages.

P7) Locate all the messages involved in the Google IP address discovery process (as DNS as ARP). Justify step by step how the process has been done.

Now follow the next steps:

1.- Open Wireshark and start a capture session using the correct network interface.

2.- Execute in a command prompt (or in a Shell under GNU Linux) the following commands:

Under Windows:

```
netsh interface ip delete arpcache  
ipconfig /flushdns
```

Under Linux:

```
sudo ip neigh flush dev eth0  
sudo /etc/init.d/nscd restart
```

3.- Ping www.google.com

4.- Stop the capture session after intercepting some ping messages.

P8) Explain what do the commands of step 2.

P9) Locate all the messages involved in the Google IP address discovery process (as DNS as ARP). What have changed from question P7? Justify your answer.

2.2.3. ARP poisoning

Open a command prompt (or in a Shell under GNU Linux) and, by using the necessary commands, add a new entry in the host ARP table so that when you ping from the host 'A' to another host 'B' in the classroom, instead of sending the message to 'B' (as would be logical), it arrives at 'A'. Capture it with Wireshark.

P10) Attach descriptive screenshots showing the new ARP table and the messages captured by Wireshark. Describe the commands used to do the ARP poisoning and justify their usage.

3. Tips and best practices

- When you need to do a capture session in Wireshark, try to have the minimum number of applications running in background (at least those which use the network) to minimize the number of messages captured.
- Use the **filter tool** implemented in Wireshark. You can check how to make filters on both the user manual of Wireshark and the online help. The use of this tool will save you a lot of time and trouble.
- Check the necessary commands (as well as their options) and make sure to have an action plan before you start doing things “like crazy”. Think what data do you need to do according to what, and think what commands can be more useful.

4. Requirements

To pass the practice is necessary to satisfy the following requirements:

- You must answer questions from all the parts of the practice.
- Answers to questions must be presented in a **pdf** document through the activity enabled on *AulaGlobal 2*. The name of the file must follow this format:

RO-PCdPW-[Wireshark_lab_session]-[student_group_ID].pdf

Where *student group ID* shall be composed as follows:

XY-Z

Where:

X letter ‘L’ or ‘C’ for the campus (*Leganés* or *Colmenarejo*).

Y group (**80, 81, 82, 83, 84 or 89**).

Z team ID.

Thus a valid example would be: **RO-PCdPW-1-L81-5.pdf**

- Compressed formats are also available (zip, rar, tar.gz, 7z...) while respecting the naming format.

5. Rules

For this practice have been developed the following rules:

- The submitted document must have a cover with the team ID and the name of the students. Each question answered should be preceded by its statement.
- Practices that do not have at least half the questions correctly answered will be automatically failed, and the score will depend on the number of correct answers.
- Practices delivered after deadline will have a score of 0 points.
- Practices named following a different naming format will have a reduced score (original score without a number between 0.5 and 2.5 points).